документів. Технічний звіт “Настанови щодо використання і менеджементу послугами третьої довіреної сторони” стосується організаційних аспектів діяльності виділених центрів сертифікації віжкритих ключів.

Найбільших змін зазнав стандарт ISO/IEC 9796 “Цифровий підпис з відновленням повідомлень”. Нагадаємо, що колишній одночастинний стандарт мав бути доповнений іншими частинами. Після кількох ітерацій було вирішено, що це буде трьохчастинний стандарт. Перша частина – з використанням надлишковості, друга частина - з використаняям хєш-функцій, третя частина – на основі дискретних логарифмів. Після кількох атак, які спричиняють екзестинціальну підробку підпису, від першої частини довелося відмовитися, а в другій частині назріла необхідність зміни способу форматування.

Ряд проектів стандартів стосується подальшого розвитку і застосування базового стандарта з оцінювання засобів забезпечення безпеки інформаційних технологій (ISO/IEC 15408). В даний час проходить голосування, що стосується започаткування таких стандартів: безпека інформаційних мереж, генерування випадкових чисел, генерування простих чисел, декларування постачальників засобів захисту про їх відповідність прийнятим стандартам.

Таким чином, навіть короткий перегляд стандартів, за якими наш підкомітет приймав участь у голосуванні, показав, яка велика увага приділяється у світі питанням захисту інформаційних технологій. Розширення таких питань не може бути дивним у зв`язку з бурхливим розвитком інформаційних технологій, особливо у банківській і фінансовій сфері: використання карток для оплати послуг і товарів, електронна комерція, домашне банківське обслуговування, інтернет-технології тощо.

Слід також відмитити тенденцію, яку чітко видно у сфері стандартизації, а саме: спроби створення стандартів, які описують ідеологію застосування тих або інших принципів побудови захисту інформації в інформаційних технологіях. Замість опису конкретних алгоритмів часто надаються принципові підходи до їх побудови. Це дає змогу дуже гнучкого використання таких стандартів для побудови системи захисту інформаційних технологій.

Така тенденція у розвитку міжнародних стандартів може бути дуже корисною з точки зору побудови системи державних стандартів. Гармонізація міжнародних стандартів в галузі захисту інформації і безпеки інформаційних технологій може надати можливість швидкої побудови основи для розвитку стандартизації в Україні. Такий шлях створення стандартів України є достатньо дешевим і швидким, який одночасно дозволить усунути велику кількість проблем, які вже виникали в інших державах при створенні стандартів у галузі захисту інформації і безпеки інформаційних технологій. Це зовсім не означає, що потрібно повністю копіювати міжнародні стандарти для України, але застосування найкращих з них в Україні дозволить швидко вирішити частину наших питань при побудові основ стандартизації в Україні.

УДК 006.4.2:002; 53.081:006.354

НОРМАТИВНЕ ТА МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Ярослав Юзьків, Євген Козир, Олександр Шевченко
Український науково-дослідний інститут стандартизації, сертифікації та інформатики

Анотація: **У статті розглянуто нормативні документи захисту інформації в комп’ютерних системах та метрологічне забезпечення у галузі ТЗІ, зокрема, державні стандарти України з повірочних схем для повірки засобів вимірювальної техніки, що можуть використовуватися у сфері технічного захисту інформації.**

Summary: **This article deals with normative documents of security of information in computer systems and metrological support in domain of technical security of information in particular state standards of Ukraine concerning verification schemes for verification of aids of measurement technique which way be used in sphere of technical security of information**.

Ключові слова: **інформація, стандарт, захист інформації.**

Міжнародні та міждержавні стандарти

1. Згідно з каталогом Міжнародної організації зі стандартизації ISO за станом на 01.01.1999 безпосередньо захисту інформації в комп’ютерних системах стосуються понад 50 стандартів, які розподілено в основному по таких групах:

- 35.040 «Коди і кодування інформації» - 20 стандартів;
- 35.100.01 «Взаємозв’язок відкритих систем взагалі» - 7 стандартів;

- 35.100.70 «Прикладний рівень» - 2 стандарти;
- 35.240.40 «Застосування інформаційних технологій у банківській справі» - 14 стандартів

та по деяких інших групах.

Захисту інформації в комп'ютерних системах стосуються також багато інших стандартів, які містять окремі положення чи вимоги.

2. У каталозі Міждержавних стандартів (індекс «ГОСТ») відсутні стандарти, які унормовують лише захист інформації. В той же час стандартів «ГОСТ», які містять окремі положення чи вимоги щодо захисту інформації, у каталозі міждержавних стандартів можна налічити порядку двох сотень, в тому числі стандартів обмеженого доступу.

Категорії нормативних документів у сфері ТЗІ, чинні в Україні

На сьогодні в Україні чинними є ряд нормативних документів (НД), що унормовують захист інформації в комп'ютерних системах. Це документи таких категорій.

1. Закони України:

«Про інформацію»;

«Про захист інформації в автоматизованих системах»;

«Про науково-технічну інформацію»;

«Про державну таємницю»

2. Інші НД органів державної влади:

«Концепція (основи державної політики) національної безпеки України»

«Концепція технічного захисту інформації в Україні»

«Положення про порядок здійснення криптографічного захисту інформації в Україні»

3. Державні стандарти:

ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення;

ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт;

ДСТУ 3396.2-96 Захист інформації. Технічний захист інформації. Терміни та визначення.

4. Галузеві стандарти:

НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

НД ТЗІ 2.5-004-99 Критерії оцінювання захищеності інформації в комп'ютерних системах від несанкціонованого доступу;

НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функційні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

НД ТЗІ 3.7-001-99 Методичні вказівки щодо розроблення технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

Перспективи розроблення НД згідно з Програмою державної стандартизації на 1998 - 2000 рр.

У Програмі державної стандартизації на 1998 - 2000 рр. є ряд тем, що унормовують захист інформації або стосуються цієї сфери. Це такі теми.

Тема **11.2.092-96** Криптографічний захист інформації. Процедури вироблення і перевірки електронного цифрового підпису (ЕЦП) на базі асиметричного алгоритму (АСКА).

Тема **11.2.093-96** Криптографічний захист інформації. Функції гешування.

Тема **11.2.094-96** Криптографічний захист інформації. Процедура криптографічного шифрування.

Тема **11.2.035-97** Банківська справа. Затверджені алгоритми для повідомлень. Алгоритм кодування даних. Гармонізація з ISO 8731-1.

Тема **11.2.036-97** Банківська справа. Управління ключами за допомогою асиметричних алгоритмів. Ч.1. Принципи, процедури і формати. Гармонізація з ISO 11166-1.

Тема **11.2.037-97** Банківська справа. Управління ключами за допомогою асиметричних алгоритмів. Ч.2. Затверджені алгоритми, які використовують RSA-криптосистеми. Гармонізація з ISO 11166-2.

Тема **11.2.038-97** Випробування програмних та апаратно-програмних засобів захисту інформації. Загальні вимоги.

Тема **11.1.041-98** Охорона державної таємниці. Терміни та визначення.

Тема **11.2.032-99** Інформаційні технології. Інформаційна безпека. Терміни та визначення.

Зазначимо, що на сьогодні жодне відомство не бере на себе повноваження замовника цих стандартів. Отже, вони не фінансуються і не розробляються.

Дотримання єдиної державної політики у сфері стандартизації

Дотримання єдиної державної політики у сфері стандартизації здійснюється через державну реєстрацію нормативних документів різних категорій в УкрНДІССІ Держстандарту України.

Під час державної реєстрації виконується (у мінімальному обсязі) експертиза галузевих стандартів:

- правильність побудови назви нормативного документа;
- відповідність змісту НД його категорії, виду, рівню прийняття;
- правильність побудови і оформлення НД;
- несуперечливість положень НД чинним державним стандартам.

Ці функції не може виконати Мінюст: це повноваження Держстандарту України і його науково-дослідної установи.

Постанова Кабінету Міністрів від 26.06.96 №677, надаючи право затвердження Положення про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих НД системи ТЗІ, не скасувала Декрет Кабінету Міністрів України «Про стандартизацію і сертифікацію» в частині реєстрації галузевих НД ТЗІ, а отже вони підлягають державній реєстрації.

Приклади.

1. Неправильна назва НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функційні профілі захищеності оброблюваної інформації від несанкціонованого доступу». На нашу думку, назва повинна бути такою: «Стандартні функційні профілі захищеності оброблюваної інформації в автоматизованих системах від несанкціонованого доступу та класифікація їх за ступенем захищеності», оскільки основою класифікації АС є їхні функційні можливості, а ступінь захищеності є лише однією з ознак класифікації, причому, не найпріоритетнішою.

2. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» містить загальнонаукові та загальнотехнічні терміни, визначення яких подано лише стосовно їх захищеності. Це свідчить про неправильну побудову НД: загальнонаукові та загальнотехнічні терміни слід або виділити в окремий розділ з зазначенням відповідних положень чи коментарів, або подавати у супроводі сфери поширення терміна. Наприклад, комп'ютерною системою не може називатися «подана для оцінювання сукупність програмно-апаратних засобів».

Тому розроблені ДСТС ТЗІ СБУ нормативні документи ТЗІ за змістом і правилами оформлення є галузевими стандартами, які підлягають державній реєстрації в Держстандарті України згідно з п. 3 ст. 6 Декрету Кабінету Міністрів України «Про стандартизацію і сертифікацію» (від 10.05.93 № 46-93 зі змінами, внесеними Законом України від 11.06.97 №333/97-ВР). Зареєстрованим галузевим НД надається чинність як галузевим стандартам, вони заносяться в усі каталоги та довідники.

НД ТЗІ, розроблені ДСТС ТЗІ СБУ, можуть бути основою для розробки відповідних державних стандартів.

ТЗІ - проблема технічна

Технічний захист інформації - проблема технічна, і її повинні вирішувати спеціалісти наукових та дослідно-конструкторських установ і технічних комітетів зі стандартизації, зокрема, ТК 20 «Інформаційні технології», ТК 105 «Банківські та фінансові системи і технології», ТК 107 «Захист інформації».

Щодо ТК 20: органи влади не залучають спеціалістів цього комітету до розв'язання проблем захисту інформації, відповідно його спеціалістами не розроблено жодного НД у сфері захисту інформації.

Щодо ТК 105: Національний банк України залучив цей комітет до роботи над проектами стандартів, що стосуються лише фізичного захисту матеріальних цінностей, в т. ч. машинних носіїв інформації.

Щодо ТК 107, слід зауважити, що комітет фактично не працює, і слід вжити заходи щодо поновлення і обновлення його діяльності.

Питання метрологічного забезпечення у сфері ТЗІ

Як зазначено у ДСТУ 2226-93 та ДСТУ 3398.2-97, **інформація –** *це відомості про суб'єкти, об'єкти, явища та процеси.* З точки зору метрології, під інформацією про об'єкти слід розуміти фізичні величини, які характеризують об'єкти та підлягають вимірюванню. Ця інформація відображається та вимірюється за допомогою одиниць фізичних величин. Перелік цих величин наведено у стандартах ДСТУ 3651.0-97, ДСТУ 3651.1-97, ДСТУ 3651.2-97. Наприклад, це величини простору і часу та похідні одиниці, одиниці механіки, теплоти, світла та споріднених типів електромагнітного випромінювання, акустики, фізичної хімії та молекулярної фізики, атомної фізики та ін. Інформація у сфері ТЗІ повинна бути стандартизована, як це вимагає Закон «Про метрологію та метрологічну діяльність». Прилади, за допомогою яких забезпечується технічний

захист інформації та ті, які визначають придатність об'єкту до використання, повинні проходити державні приймальні випробування, метрологічну атестацію, повірку та калібрування згідно з чинними нормативними документами та чинними в Україні повірочними схемами і процедурами.

В Україні на сьогодні затверджено 37 повірочних схем, які можуть бути використанні для метрологічного забезпечення приладів у сфері ТЗІ, таблиця 1.

Перелік повірочних схем ***Таблиця 1.***

Розділ фізики по ДСТУ 3651.1-97	**Назва розділу**	**Державний стандарт України**	**Фізичні величини та метрологічні характеристики**
1	Простір та час	ДСТУ 3538-97	Інтервали часу, діапазон від $1\bullet10^{-10}$ до $1\bullet10^{8}$ с, частота від 1 до $7\bullet10^{10}$ Гц
		ДСТУ 3537-97	Об'єм рідини від $1\bullet10^{-3}$ до 1 $м^3$
		ДСТУ 3497-97	Рівень рідини від 0 до 20 м
2	Періодичні та пов'язані з ними явища	ДСТУ 3741-98	Довжина від $1\bullet10^{-6}$ до 50 м, довжина хвиль від 0,2 до 50 мкм
3	Механіка	ДСТУ 3381-96	Маса 1 кг; ціна поділки ваг $4\bullet10^{-2}$ мг
		ДСТУ 3385-96	Параметри евольвентних поверхонь та куту нахилу зуба радіусу від 37 до 150 мм з кутами розгорнутості від 0^o до 35^o
		ДСТУ 3386-96	Відхилення від прямолінійності та площинності 0,3 мкм
		ДСТУ 3382-96	Прискорення сили ваги від 977 до 985 Гал (1 Гал=$1\bullet10^{-2}$ $м/с^2$)
		ДСТУ 3388-96	Абсолютний тиск в діапазоні від $1\bullet10^{-6}$ до $1\bullet10^{3}$ Па
		ДСТУ 3496-97	Абсолютний тиск від $2,7\bullet10^{2}$ до $4\bullet10^{5}$ Па
		ДСТУ 3383-96	Об'єм та об'ємна витрата газу від $1,11\bullet10^{-3}$ до $5,55\bullet10^{-2}$ $м^3/с$
		ДСТУ 3869-99	Твердість за шкалою Роквелла від 70 до 93 HRA, від 25 до 100 HRB, від 20 до 67 HRC; твердість за шкалою Супер-Роквелла від 70 до 94 HRN 15, від 40 до 86 HRN 30, від 20 до 78 HRN 45, від 62 до 93 HRT 15, від 215 до 82 HRT 30, від 10 до 72 HRT 45
		ДСТУ 3870-99	Твердість за шкалою Брінелля від 8 до 450 HB, від 95 до 650 HBW; твердість за шкалою Віккерса від 8 до 2000 HV
4	Теплота	ДСТУ 2614-94	Енергія згоряння від 25 до 35 кДж
		ДСТУ 3194-95	Температура (за випромінюванням) від мінус 50 до 100000 ^oC
		ДСТУ 3742-98	Температура (контактна) від 13,8 до 2800 К
5	Електрика та магнетизм	ДСТУ 3384-96	Потужність електромагнитних коливань у хвилеводних трактах від $1\bullet10^{-3}$ до $1\bullet10^{-2}$ Вт, в діапазоні частот від 37,5 до 178,6 ГГц
		ДСТУ 3390-96 (ГОСТ 8.144-97)	Магнітна індукція постійного магнітного поля в діапазоні від 0,05 до 2 Тл
		ДСТУ 3393-96 (ГОСТ 8.109-97)	Коефіцієнт амплітудної модуляції високочастотних коливань у діапазоні від 0,1 % до 100 % у діапазоні частот носіїв від 0,01 до 500 МГц, модулювальних частот від 0,02 до 200 кГц
		ДСТУ 3391-96 (ГОСТ 8.110-97)	Коефіцієнт гармонік від 0,003 % до 100% в діапазоні частот першої гармоніки від 10 Гц до 200 кГц
		ДСТУ 3712-98	Опір від 1 до 100 Ом, мір електричного опору від $1\bullet10^{-3}$ до $1\bullet10^{9}$ Ом

Розділ фізики по ДСТУ 3651.1-97	**Назва розділу**	**Державний стандарт України**	**Фізичні величини та метрологічні характеристики**
		ДСТУ 3864-99	Напруга змінного струму від 1 до 1,2 •500/√ 3 кВ, коефіцієнт масштабного перетворення напруги на частоті 50 Гц
		ДСТУ 3863-99	Напруга постійного струму від 1 до 800 кВ
		ДСТУ 3834-98	Електрорушійна сила (ЕРС) та постійна напруга від 0,01 до 1 В
		ДСТУ 3392-96 (ГОСТ 8.232-97)	Девіація частоти від 10 до 10^6 Гц в діапазоні частот модулювальних сигналів від 0,02 до 200 кГц та в діапазоні частот сигналів носіїв від 0,1 до 10000 МГц
		ДСТУ 3391-96	Коефіцієнт гармонік в діапазоні значень від 0,003% до 1000% та в діапазоні частот першої гармоніки від 10 Гц до 200 кГц
		ДСТУ 3384-96	Потужність електромагнітних коливань від 37,5 до 178,6 ГГц
6	Світло та споріднені типи електромагнітного випромінювання	ДСТУ 3193-95	Енергетична освітленість некогерентним випромінюванням
		ДСТУ 3395-96	Енергетична освітленість від 10^{-5} до 1 Вт/м^2 в діапазоні довжин хвиль від 0,2 до 50 мкм
		ДСТУ 3539-97	Середня потужність лазерного випромінювання та енергія лазерного випромінювання від $1•10^{-4}$ до 1 Вт у діапазоні хвиль від 0,3 до 12,0 мкм
		ДСТУ 3387-96	Потужність слабких імпульсних світлових потоків випромінювання від 10^{-6} до 10^{-2} Вт в діапазоні хвиль від 0,4 до 1,6 мкм
		ДСТУ 3394-96	Сила світла від 30 до 100 кд; освітленість від 1 до $2•10^5$ лк, яскравості від $1•10^{-1}$ до $1•10^{10}$ кд/м^2
		ДСТУ 3193-95	Освітленість некогерентним випромінюванням від 10 до 10^{-5} Вт/м^2
		ДСТУ 3387-96	Потужність слабких імпульсних потоків випромінювання від $1•10^{-6}$ до $1•10^{-2}$ Вт в діапазоні довжин хвиль від 0,4 до 1,6 мкм
7	Акустика		
8	Фізична хімія та молекулярна фізика	ДСТУ 3214-95	Концентрація компонентів у газових середовищах (11 компонентів)
9	Атомна та ядерна фізика	ДСТУ 3743-98	Активність α-випромінювання від 5 до $5•10^{12}$ Бк, β-випромінювання від 5 до $5•10^{12}$ Бк, αγ-βγ-випромінення від 10^2 до 10^6 Бк, γ-випромінювання від $1•10^6$ до $5•10^{12}$ Бк; питома активність та об'ємна активність радіонуклідів
		ДСТУ 3536-97	Об'ємна активність радона-222 у повітрі від 1,0 до 5 $•10^4$ Бк •м$^{-3}$
10	Ядерні реакції та йо-нізувальні випромінювання		
11	Фізика твердого тіла		

Таким чином, по багатьох розділах фізики мало еталонів та повірочних схем, а по деяких зовсім немає. Це стосується у першу чергу акустичних, електромагнітних та оптичних вимірювань.

Вимоги до об'єктів, підпорядкованих ТЗІ, мають перевірятися приладами з досить високою чутливістю.

Порогова чутливість та роздільна здатність існуючих приладів явно недостатня для використання у сфері ТЗІ. І в першу чергу недостатньо засобів ТЗІ, які стосуються вимірювання параметрів фізичних величин на відстані від об'єкту.

Бажано ввести таке поняття та термін, як **піднаглядність об'єкта вимогам ТЗІ**, як це існує наприклад у такій сфері стандартизації, як охорона праці; у метрології – державний метрологічний контроль, державний метрологічний нагляд.

При проектуванні приладів з ТЗІ слід відрізняти такі поняття, як технічна характеристика, метрологічна характеристика, точнісна характеристика.

Необхідно розрізняти поняття: *одиниця фізичної величини*, *одиниця вимірювання*, *метрологічна характеристика;* а також: *коефіцієнт*, *параметр*, *фактор*.

Висновок. Для розвитку сфери використання технічних засобів ТЗІ необхідно розширити кількість еталонів та повірочних схем, підвищити чутливість приладів.

УДК 638.235.231

ЛИЦЕНЗИРОВАНИЕ, СЕРТИФИКАЦИЯ, ИСПЫТАНИЯ В ОБЛАСТИ ТЗИ В УКРАИНЕ

Александр Лаврентьев
НИЦ "ТЕЗИС" НТУУ "КПИ"

Аннотация: **В настоящей статье изложена точка зрения специалиста по ПД ТСР на формирование системы лицензирования и сертификации в области ТЗИ в Украине.**
Summary: **In this article of the specialists of counteraction of TMSS presents his point of view on the formation of the licence and sertification system in the field of TDI in Ukraine.**
Ключевые слова: **Лицензирование, сертификация, испытания.**

Одним из первых реальных шагов в формировании национальной системы ТЗИ в Украине явилось создание системы государственного лицензирования деятельности в области защиты информации. Были внесены соответствующие изменения в Закон о предпринимательской деятельности и введена в действие соответствующая инструкция. Несколько лет функционирования этой системы позволяют подвести некоторые итоги. Прежде всего необходимо установить, какие цели преследует лицензирование в области ТЗИ и достигнуты ли они? Одной из основных задач института лицензирования вообще является защита страны и ее населения от товаров, которые могут нанести ущерб жизни и здоровью граждан, экологии, нормальной работе важных систем и т.д. Целью лицензирования может служить также пополнение бюджета государства (как форма "скрытого налога" на высокодоходные виды деятельности). Обе эти цели маловероятны, так как деятельность в области ТЗИ не проносит сверхприбылей, цена лицензии не высока, а угрозы для здоровья и экологии отсутствует.

Можно сделать вывод, что лицензирование предпринимательской деятельности в области защиты информации с ограниченным доступом от утечки по техническим каналам может иметь смысл как государственная гарантия качества предоставляемых услуг. Это существенно при проведении мероприятий по защите гостайны. Но для тех, кто работает с гостайной, давно существует налаженный механизм допуска и при отсутствии такого, надлежащим образом оформленного, никакая лицензия не даст права на проведение работ по защите секретной информации. Несколько иная ситуация возникает при организации защиты информации субъектами негосударственного сектора. При этом наблюдаются два подхода к решению проблемы.

В первом случае руководство субъекта предпринимательской деятельности (далее фирма) понимает необходимость защиты информации и реально заинтересовано в качественном выполнении работ. При этом фирма будет искать специалистов, имеющих наибольший авторитет в данной области, не зависимо от того, работают ли специалисты в организации, имеющей лицензию. Таким образом, стимулируется проведение этих работ за счет теневого сектора экономики. Не исключено, что коммерческие структуры не всегда охотно пойдут на сотрудничество с лицензиатами, находящимися под прямым контролем СБУ.

Во втором случае руководство фирмы не считает актуальным необходимость проведения мероприятий по защите информации, но желает выполнить все положенные требования. В этой ситуации для заказчика не имеет значения качество выполнения работ, важно только, чтобы договор и результаты работ были оформлены в соответствии с требованиями руководящих документов (кстати, аналогичное отношение в ряде случаев просматривается и в госучреждениях). Такой подход дискредитирует систему ТЗИ вообще и лицензирования деятельности в этой области в частности. Кроме того, в этой ситуации снижаются требования к линцезиатам, что понижает общий уровень проведения работ в области ТЗИ в целом по стране.